IntroductionMechanicsUseful LinksExamples / JobsPascal's Triangle<br/>ocFast MultiplicationEuclidean AlgorithmFermat's little<br/>occoord

# Math 317: Operations Research First Lecture

Steven J Miller Williams College

### sjm1@williams.edu

http://www.williams.edu/Mathematics/sjmiller/public\_html/317

Williams College

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
0000							

Introduction and Objectives

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
0000							

### Introduction / Objectives

# Main Topic: Optimization: Linear Programming.

# Objectives

- Obviously learn linear programming.
- Emphasize techniques / asking the right questions.
- Model problems and analyze model.
- Elegant solutions vs brute force.
- Writing textbook for AMS.

Introduction Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
0000 0000						

# **Types of Problems**

- Diet problem.
- Banking (asset allocation).
- Scheduling (movies, airlines, TSP, MLB).
- Elimination numbers.
- Sphere packing....

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
0000							

### My (applied) experiences

- Marketing: parameters for linear programming (SilverScreener).
- Data integrity: detecting fraud with Benford's Law (IRS, Iranian elections).
- Sabermetrics: Pythagorean Won-Loss Theorem.



Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
	0000						

# **Course Mechanics**

Introduction		Pascal's Triangle	Euclidean Algorithm	Fermat's littl 000000

## Grading / Administrative

- HW: 15%. Midterm 40%. Final/Project 40%. Class Participation 5%. May change a bit. A large portion of work/grade from a group project: you'll give a talk, prepare a well-crafted manuscript, and respectfully listen to reports of others.
- Pre-reqs: linear algebra (analysis, stats, programming a plus).

# Office hours / feedback

- TBD and when I'm in my office (schedule online).
- Feedback ephsmath@gmail.com, password first 8 Fibonacci numbers (011235813).

Introduction	Mechanics ○○●○	Useful Links oo	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
Other							

- Webpage: numerous handouts, additional comments each day (mix of review and optional advanced material).
- Opportunity to help write a book.
- PREPARE FOR CLASS! Must do readings before each class.



Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
	0000						

# • Party less than the person next to you.

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
	0000						

- Party less than the person next to you.
- Take advantage of office hours / mentoring.

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
	0000						

- Party less than the person next to you.
- Take advantage of office hours / mentoring.
- Learn to manage your time: no one else wants to.

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
	0000						

- Party less than the person next to you.
- Take advantage of office hours / mentoring.
- Learn to manage your time: no one else wants to.

Happy to do practice interviews, adjust deadlines....

Linear algebra textbooks online: http: //joshua.smcvt.edu/linalg.html/book.pdf

Introduction Mech	anics Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
	••					

# Useful links

Introduction Mechanics Useful Links Examples / Jobs Pascal's Triangle Fast Multiplication Euclidean Algorithm Fermat's little occord

### LaTeX and Mathematica Tutorials and Templates

http://web.williams.edu/Mathematics/sjmiller/public\_html/math/handouts/latex.htm

# Has templates for using LaTeX for papers, talks, posters, and a Mathematica tutorial.

Also videos on each.

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			00000				

# Examples / Jobs

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			00000				

### Alabama vs Auburn: 2013

https: //www.youtube.com/watch?v=sLO2SmM9gPw

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			000000				

# Log ruler (and WCMA)



Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			00000				

# Log ruler (and WCMA)



Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			000000				

### Log ruler (and WCMA)

#### 11.2014.26.62

As New England forests became depleted in the nineteenth century, lumber companies surveyed their trees more carefully to ensure profit. With this two-foot scale, a man called a "scaler" could estimate the usable output of wood. Lumberjacks distrusted the mathematically trained scaler in protection of their daily wages, which were based on individual production. Introduction Mechanics Useful Links Examples / Jobs Pascal's Triangle Fast Multiplication Euclidean Algorithm Fermat's littl

### Scheduling: Baseball Tournaments, Swim Lessons

Introduction

000000

Mechanics Useful Links Examples / Jobs Pascal's Triangle Fast Multiplication Euclidean Algorithm Fermat's littl

## Scheduling: Baseball Tournaments, Swim Lessons



Introduction

000000

Mechanics Useful Links Examples / Jobs Pascal's Triangle Fast Multiplication Euclidean Algorithm Fermat's littl

## Scheduling: Baseball Tournaments, Swim Lessons



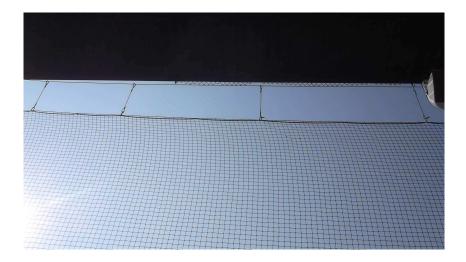
Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			000000				



Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			000000				



Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			000000				



Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			000000				



Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			000000				

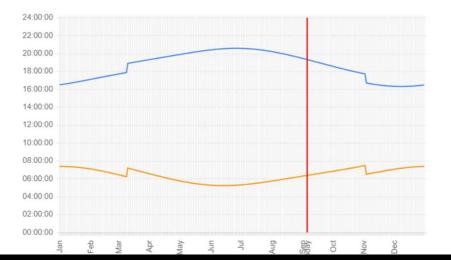
	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Y			1 Aliones Fund & Bornti Fand bege	2	3	4	S Max Ranson Feetbad Washind
	e	5 7	8	9	10	11	12
		Eid al-Adha (begats at sandown) Columbus Day	Tal al-Adha Badig Penal eade	16	17	18	19
	20	21	22	23	24	25 8 Farmiy Westand	26
	27	28	29	30	31 8 9 22	SEPTEMBER 13   M T W T F S   2 3 4 5 6 7   9 10 11 12 13 14   6 16 17 18 19 20 21   2 32 24 25 26 27 28	SMTWTER

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
			000000				



						Euclidean Algorithm	
0000	0000	00	000000	00	00000	000	000000
Mane							

### Year distribution of sunrise and sunset times in North Adams, MA – 2019 https://sunrise – sunset.org/us/north – adams – ma



# Who America is rooting for in the Super Bowl:



Maps

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
				•0			

# Pascal's Triangle

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
				00			

### **Pascal's Triangle**

# Video on Pascal's Triangle

https: //www.youtube.com/watch?v=tt4\_4YajqRM

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
					00000		

# Fast Multiplication

Introduction Mechanics Useful Links Examples / Jobs Pascal's Triangle **Fast Multiplication** Euclidean Algorithm Fermat's littl

### **Cost of Standard Polynomial Evaluation**

Multiplication far more expensive than addition....

$$f(x) = 3x^5 - 8x^4 + 7x^3 + 6x^2 - 9x + 2$$
: Cost is   
5 + 4 + 3 + 2 + 1 + 0 = 15 multiplications.

These are triangle numbers: degree *d* have d(d+1)/2.

Introduction Mechanics Useful Links Examples / Jobs Pascal's Triangle Fast Multiplication euclidean Algorithm Fermat's little

### **Cost of Standard Polynomial Evaluation**

Multiplication far more expensive than addition....

$$f(x) = 3x^5 - 8x^4 + 7x^3 + 6x^2 - 9x + 2$$
: Cost is   
5 + 4 + 3 + 2 + 1 + 0 = 15 multiplications.

These are triangle numbers: degree *d* have d(d+1)/2.

$$S(d) = 1 + 2 + \cdots + d$$
  
 $S(d) = d + (d - 1) + \cdots 1$ 

Introduction Mechanics Useful Links Examples / Jobs Pascal's Triangle Fast Multiplication euclidean Algorithm Fermat's little

### **Cost of Standard Polynomial Evaluation**

Multiplication far more expensive than addition....

$$f(x) = 3x^5 - 8x^4 + 7x^3 + 6x^2 - 9x + 2$$
: Cost is   
5 + 4 + 3 + 2 + 1 + 0 = 15 multiplications.

These are triangle numbers: degree *d* have d(d+1)/2.

$$S(d) = 1 + 2 + \dots + d$$
  
 $S(d) = d + (d - 1) + \dots 1$ 

Thus  $2S(d) = d \cdot (d+1)$  and claim follows.

Introduction		Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
Hornei	r's Algo	orithm					

$$f(x) = 3x^5 - 8x^4 + 7x^3 + 6x^2 - 9x + 2$$
: Cost is   
5 + 4 + 3 + 2 + 1 + 0 = 15 multiplications.

Horner's algorithm:

$$\left(\left(\left((3x-8)x+7\right)x+6\right)x-9\right)x+2$$

Introduction	Mechanics 0000		Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
Horne	r's Algo	orithm					

$$f(x) = 3x^5 - 8x^4 + 7x^3 + 6x^2 - 9x + 2$$
: Cost is   
5 + 4 + 3 + 2 + 1 + 0 = 15 multiplications.

Horner's algorithm:

$$\left(\left(\left((3x-8)x+7\right)x+6\right)x-9\right)x+2$$

Cost is degree d multiplications!

Useful also in fractal plotting.... Shows can often do common tasks faster.

Introduction		Useful Links	Pascal's Triangle	Fast Multiplication ○○○●○	Euclidean Algorithm	Fermat's littl
Fast M	ultiplic	ation				

Horner is best in general, but maybe for special polynomials can do better?

Try polynomials of the form f(x) =



Horner is best in general, but maybe for special polynomials can do better?

Try polynomials of the form  $f(x) = x^n$ .



Horner is best in general, but maybe for special polynomials can do better?

Try polynomials of the form  $f(x) = x^n$ .

$$egin{array}{rcl} x \cdot x &=& x^2 \ x^2 \cdot x^2 &=& x^4 \ x^4 \cdot x^4 &=& x^8 \ x^8 \cdot x^8 &=& x^{16} \ x^{16} \cdot x^{16} &=& x^{32} \ x^{32} \cdot x^{32} &=& x^{64} \end{array}$$



Horner is best in general, but maybe for special polynomials can do better?

Try polynomials of the form  $f(x) = x^n$ .

$$\begin{array}{rcrcrcrc} x \cdot x &=& x^2 \\ x^2 \cdot x^2 &=& x^4 \\ x^4 \cdot x^4 &=& x^8 \\ x^8 \cdot x^8 &=& x^{16} \\ x^{16} \cdot x^{16} &=& x^{32} \\ x^{32} \cdot x^{32} &=& x^{64} \end{array}$$



Horner is best in general, but maybe for special polynomials can do better?

Try polynomials of the form  $f(x) = x^n$ .

$$\begin{array}{rcrcrcrc} x \cdot x &=& x^2 \\ x^2 \cdot x^2 &=& x^4 \\ x^4 \cdot x^4 &=& x^8 \\ x^8 \cdot x^8 &=& x^{16} \\ x^{16} \cdot x^{16} &=& x^{32} \\ x^{32} \cdot x^{32} &=& x^{64} \end{array}$$



Horner is best in general, but maybe for special polynomials can do better?

Try polynomials of the form  $f(x) = x^n$ .

$$\begin{array}{rclrcrcrc} x \cdot x & = & x^2 \\ x^2 \cdot x^2 & = & x^4 \\ x^4 \cdot x^4 & = & x^8 \\ x^8 \cdot x^8 & = & x^{16} \\ x^{16} \cdot x^{16} & = & x^{32} \\ x^{32} \cdot x^{32} & = & x^{64} \end{array}$$

Introduction	Useful Links oo	Examples / Jobs	Pascal's Triangle	Fast Multiplication ○○○○●	Euclidean Algorithm	Fermat's littl
Recap						

Horner takes us from order  $d^2$  to order d.

Fast multiplication takes us to order  $\log_2 d$ , but only for special polynomials; these though are the ones used in RSA!

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
						000	

# **Euclidean Algorithm**

Introduction		Pascal's Triangle	Euclidean Algorithm	Fermat's littl

## **Preliminaries**

Input x, y with y > x.

Goals: find gcd(x, y), find a, b so that ax + by = gcd(x, y).

Lot of ways to go: non-constructive proofs of *a*, *b* but need values; Euclidean algorithm is *very* fast.

Introduction	Mechanics 0000	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm ○○●	Fermat's littl
Euclid	ean Alg	gorithm					

Let 
$$r_0 = y, r_1 = x$$
.

$$r_0 = q_1 r_1 + r_2, \quad 0 \le r_2 < r_1.$$

Introduction 0000	Mechanics 0000		Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm ○○●	Fermat's littl
Euclid	ean Alg	gorithm					

Let 
$$r_0 = y, r_1 = x$$
.

$$r_0 = q_1 r_1 + r_2, \quad 0 \le r_2 < r_1.$$

$$r_1 = q_2 r_2 + r_3, \quad 0 \le r_3 < r_2.$$

Introduction			Pascal's Triangle	Euclidean Algorithm ○○●	Fermat's littl
Euclid	ean Ald	norithm			

Let 
$$r_0 = y, r_1 = x$$
.

$$r_0 = q_1 r_1 + r_2, \quad 0 \le r_2 < r_1.$$

$$r_1 = q_2 r_2 + r_3, \quad 0 \leq r_3 < r_2.$$

Continue until....

 $r_n = q_{n+1}r_{n+1} + r_{n+2}, r_{n+2} \in \{0, 1\}.$ 

Introduction	Mechanics 0000	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
Euclide	ean Alo	orithm					

Let 
$$r_0 = y, r_1 = x$$
.

$$r_0 = q_1 r_1 + r_2, \quad 0 \le r_2 < r_1.$$

$$r_1 = q_2 r_2 + r_3, \quad 0 \le r_3 < r_2.$$

# Continue until....

$$r_n = q_{n+1}r_{n+1} + r_{n+2}, r_{n+2} \in \{0, 1\}.$$

Note  $gcd(r_0, r_1) = gcd(r_1, r_2) = gcd(r_2, r_3), \ldots$ 

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
Euclide	ean Alg	gorithm					

Let 
$$r_0 = y, r_1 = x$$
.

$$r_0 = q_1 r_1 + r_2, \quad 0 \le r_2 < r_1.$$

$$r_1 = q_2 r_2 + r_3, \quad 0 \le r_3 < r_2.$$

Continue until....

$$r_n = q_{n+1}r_{n+1} + r_{n+2}, r_{n+2} \in \{0, 1\}.$$

Note  $gcd(r_0, r_1) = gcd(r_1, r_2) = gcd(r_2, r_3), \ldots$ 

Can 'climb upwards' to get a, b such that ax + by = gcd(x, y).

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
							00000

# Fermat's little Theorem

Introduction		Useful Links		Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
Euler t	otient f	functior	1				

 $\phi(n)$  is the number of integers from 1 to *n* relatively prime to *n*.

$$\phi(p) = p - 1$$
 and  $\phi(pq) = (p - 1)(q - 1)$  if  $p, q$  distinct primes.

Do not need, but  $\phi(mn) = \phi(m)\phi(n)$  if gcd(m, n) = 1, and  $\phi(p^k) = p^k - p^{k-1}$ .

A lot of group theory lurking in the background, only doing what absolutely need.

Introduction	Mechanics	Useful Links	Examples / Jobs	Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl
							000000

#### Fermat's little Theorem

## Fermat's little Theorem (FIT)

Let *a* be relatively prime to *n*. Then  $a^{\phi(n)} = 1 \mod n$ .

Special cases:  $a^{p-1} = 1 \mod p$ ,  $a^{(p-1)(q-1)} = 1 \mod pq$ .

Will only prove these two cases....

			Examples / Jobs	Fast Multiplication	Euclidean Algorithm	Fermat's littl
Droof	of Earm	aat'a litt	le Theorei			

**Proof:** Let n = p, let gcd(a, p) = 1.

Consider 1, 2, ..., p - 1 and a, 2a, ..., (p - 1)a.

Claim both sets are all residues modulo p.



**Proof:** Let n = p, let gcd(a, p) = 1.

Consider 1, 2, ..., p - 1 and a, 2a, ..., (p - 1)a.

Claim both sets are all residues modulo *p*.

If  $ia = ja \mod p$  then  $(i - j)a = 0 \mod p$  so  $i = j \mod p$ .



## **Proof of Fermat's little Theorem:** n = p

**Proof:** Let n = p, let gcd(a, p) = 1.

Consider 1, 2, ..., p - 1 and a, 2a, ..., (p - 1)a.

Claim both sets are all residues modulo *p*.

If  $ia = ja \mod p$  then  $(i - j)a = 0 \mod p$  so  $i = j \mod p$ . Thus  $(p - 1)! = (p - 1)!a^{p-1} \mod p$ , so  $a^{p-1} = 1 \mod p$ .  $\Box$  

### **Proof of Fermat's little Theorem:** n = p

**Proof:** Let n = p, let gcd(a, p) = 1.

Consider 1, 2, ..., p - 1 and a, 2a, ..., (p - 1)a.

Claim both sets are all residues modulo *p*.

If  $ia = ja \mod p$  then  $(i - j)a = 0 \mod p$  so  $i = j \mod p$ . Thus  $(p - 1)! = (p - 1)!a^{p-1} \mod p$ , so  $a^{p-1} = 1 \mod p$ .  $\Box$ 

Note: General case:  $x_1, \ldots, x_{\phi(n)}$  and  $ax_1, \ldots, ax_{\phi(n)}$ .

Introduction			Examples / Jobs		Fast Multiplication	Euclidean Algorithm	Fermat's littl ○○○○●○
Proof	of Ferm	nat's litt	le Theorei	<b>m:</b> <i>n</i> = <i>pq</i>			

# **Proof:** Let n = pq, let gcd(a, pq) = 1.

Introduction 0000		Pascal's Triangle	Euclidean Algorithm	Fermat's littl ○○○○●○

### **Proof of Fermat's little Theorem:** n = pq

**Proof:** Let n = pq, let gcd(a, pq) = 1.

Apply FIT with  $a^{q-1}$  and p:  $(a^{q-1})^{p-1} = 1 \mod p$ .

Apply FIT with  $a^{p-1}$  and q:  $(a^{p-1})^{q-1} = 1 \mod q$ .

Introduction		Pascal's Triangle	Euclidean Algorithm	Fermat's littl ○○○○●○

## **Proof of Fermat's little Theorem:** n = pq

**Proof:** Let n = pq, let gcd(a, pq) = 1.

Apply FIT with  $a^{q-1}$  and p:  $(a^{q-1})^{p-1} = 1 \mod p$ .

Apply FIT with  $a^{p-1}$  and q:  $(a^{p-1})^{q-1} = 1 \mod q$ .

Thus  $a^{(p-1)(q-1)}$  is 1 mod p and is 1 mod q.

 $a^{(p-1)(q-1)} = 1 + \alpha p = 1 + \beta q.$ 

Introduction			Euclidean Algorithm	Fermat's littl ○○○○●○

## **Proof of Fermat's little Theorem:** n = pq

**Proof:** Let n = pq, let gcd(a, pq) = 1.

Apply FIT with  $a^{q-1}$  and p:  $(a^{q-1})^{p-1} = 1 \mod p$ .

Apply FIT with  $a^{p-1}$  and q:  $(a^{p-1})^{q-1} = 1 \mod q$ .

Thus  $a^{(p-1)(q-1)}$  is 1 mod p and is 1 mod q.

 $a^{(p-1)(q-1)} = 1 + \alpha p = 1 + \beta q.$ 

Thus  $\alpha p = \beta q$  so  $q | \alpha$  and  $p | \beta$ , so  $a^{(p-1)(q-1)} = 1 \mod pq$ .

Introduction		Useful Links		Pascal's Triangle	Fast Multiplication	Euclidean Algorithm	Fermat's littl ○○○○○●
Primal	ity Tes	ts from	FIT				

If gcd(a, n) = 1 and  $a^{n-1} \neq 1 \mod n$  then *n* cannot be prime.

If equalled 1 then *n* might be prime.

Introduction 0000			Pascal's Triangle	Euclidean Algorithm	Fermat's littl ○○○○○●
Drimol		CIT.			

## Primality Tests from FIT

If gcd(a, n) = 1 and  $a^{n-1} \neq 1 \mod n$  then *n* cannot be prime.

If equalled 1 then *n* might be prime.

- If can take high powers, very fast!
- Can suggest candidate primes, and then use better, slower test for certainty.
- Carmichael numbers: Composites that are never rejected: 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, ... (OEIS A002997).